From AI to Dependability: using Bayesian Networks for Reliability Modeling and Analysis

Luigi Portinale, Andrea Bobbio, Stefania Montani
Dipartimento di Informatica
Universita del Piemonte Orientale "A. Avogadro"
I-15100 Alessandria
Italy
portinal@di.unipmn.it

Bayesian Networks (BN) provide a robust probabilistic method of reasoning under uncertainty. They have been successfully proposed in the field of Artificial Intelligence (AI) as the most flexible formalism for reasoning under uncertain knowledge (Neapolitan 1990; Pearl 1989; Jensen 2001). Their success stands from several factors:

- the graphical representation of the knowledge to reason with; in particular the graphical representation of the set of dependencies among the modeled variables, through the notion of *d-separation* (Pearl 1989);
- the restricted number of probabilities to be specified with respect to a complete joint probability model;
- the possibility of performing different kinds of inferences such as *prediction* (i.e. to infer information about effects starting from causes), *abduction* or *diagnosis* (i.e. to infer information about causes starting from effects) and *inter-causal reasoning* (i.e. to infer information about one cause given information about the effect and another cause);
- the possibility of "learning" the model from a database of observations.

For these reasons, they have been successfully applied in a variety of real-world tasks (Heckermann and Wellman 1995). However, they have received little attention in the area of dependability and reliability analysis. A few exceptions are the work by Almond exploiting a special kind of graphical models for modeling the reliability of a system (Almond 1992), the approach in (Torres-Toledano and Sucar 1998; Solano-Soto and Sucar 2001) where reliability block diagrams are converted into Bayesian Networks for the analysis and the recent work by Langseth (Langseth 2002).

The present talk is aimed at exploring the capabilities of the BN formalism in the modeling and analysis of dependable systems. Starting from the work described in (Portinale and Bobbio 1999; Bobbio, Portinale, Minichino, and Ciancamerla 2001), we compare BN with one of the most popular techniques for dependability analysis of large, safety critical systems, namely Fault Trees Analysis (FTA).

The talk shows that any Fault Tree (FT) can be directly mapped into a BN and that basic inference techniques on the latter may be used to obtain classical parameters computed from the former (i.e. reliability of the Top Event or of any sub-system, criticality of components, etc). The advantage is that, by using BN, some additional power can be obtained, both at the modeling and at the analysis level.

At the modeling level, several restrictive assumptions implicit in the FT methodology can be removed and various kinds of dependencies among components can be accommodated. In particular, while classical fault trees are essentially a binary formalism (i.e. dealing with binary events like 'component up' or 'component down'), Bayesian nets deals with multi-state variables, by allowing for example the modeling of different behavioral modes of a given system component.

This is very important when different kind of faults of the same component may lead to different malfunction in the whole system; incorporating such a feature into FTA requires a major modification of

the basic framework (see (Garribba, Guagnini, and Mussio 1985; Doyle, Dugan, and Patterson-Hine 1995; Wood 1985)), while it is extremely natural by using BN, where also sequentially dependent failures can be contextually modeled (Bobbio, Portinale, Minichino, and Ciancamerla 2001; Bobbio, Franceschinis, Gaeta, Portinale, Minichino, and Ciancamerla 2003).

Moreover, while in FTA logical dependency between components can only be modeled through logical gates (AND/OR gates or similar), noisy probabilistic gates can be naturally introduced and modeled by using a BN, as well as the incorporation in the model of *common cause failures*, *coverage* or similar dependencies.

At the analysis level, classical quantitative analysis can be easily performed by querying the network for the probability of the Top Event node being true. On the other hand, general BN inference is able to return the joint probability of any set of variables, given that some variables of the net have been observed (evidence variables). This means that a general diagnostic analysis can be performed, by computing arbitrary posterior probabilities; for instance, it is possible to estimate the real criticality of a component, by asking for the posterior probability of its failure, given the the Top Event has occurred. Moreover, posterior analysis can provide what is called the Most Probable Explanation (MPE) of a fault, by providing the most probable configuration of system components given that a fault has occurred (Portinale and Bobbio 1999; Bobbio, Portinale, Minichino, and Ciancamerla 2001).

The above aspects will be presented by considering some real-world examples and applications ranging from the control of multiprocessor computer systems, to the analysis of the reliability of digital controllers (industrial PLCs, turbin control systems, etc...) (Portinale and Bobbio 1999; Bobbio, Portinale, Minichino, and Ciancamerla 2001; Bobbio, Franceschinis, Gaeta, Portinale, Minichino, and Ciancamerla 2003).

We will finally report on some work in progress concerning the use of formalisms extending BN to a parametric representation (particularly useful when modeling systems with several redundant components) (Bobbio, Montani, and Portinale 2003). This is in line with a similar work presented in (Bangsø and Wuillemin 2001) where Object-Oriented Bayesian Networks are used in order to introduce classes of nodes with similar instances, while in (Bobbio, Montani, and Portinale 2003) we investigated the possibility of exploiting Probabilistic Horn Abduction (Poole 1994), a logical formalism extending Baysian Networks from a propositional to a (restricted) first-order language.

Another extension we are currently dealing with is the use of Dynamic Bayesian Networks (DBN) when modeling so-called dynamic gates (Montani, Portinale, and Bobbio 2004). We show how BN can provide a unified framework in which also *Dynamic* FT (DFT) (Dugan, Bavuso, and Boyd 1992; Dugan, Bavuso, and Boyd 1993; Manian, Coppit, Sullivan, and Dugan 1999), a recent extensions able to treat complex types of dependencies, can be represented. Dynamic Fault Trees introduce four basic (dynamic) gates: the warm spare, the sequence enforcing, the probabilistic dependency and the priority AND. DFT are typically solved by automatic conversion to the equivalent Markov model (Dugan, Bavuso, and Boyd 1992). Through a process known as modularization (Bobbio and Raiteri 2004; Dugan, Sullivan, and Coppit 2000) it is possible to identify the independent subtrees with dynamic gates and use a different Markov model (much smaller than the model corresponding to the entire FT) for each of them. Nevertheless, there still exists the problem of state explosion, since the set of states can be significantly large.

In order to overcome these limitations, we discuss how to characterize dynamic gates within the Dynamic Bayesian Network framework, where a factorized representation of a Markov Chain is adopted. We provide a translation of dynamic gates into a DBN, by comparing the approach to standard Markov chain representation of the gates. We also present the reliability analysis of a real-world system (a cardiac assist device presented in (Ou and Dugan 2000)); results demonstrate how DBN can be safely exploited for quantitative analysis, as well as for enhancing modeling and analysis of the given system (Montani, Portinale, and Bobbio 2004).

References

Almond, R. (1992). An extended example for testing Graphical Belief. Technical Report 6, Statistical Sciences Inc.

Bangsø O. and P. Wuillemin (2001). Top-down construction and repetitive structures representation in bayesian networks. In *proc. 13th FLAIRS*, Key West, pp. 340–344.

Bobbio, A., G. Franceschinis, R. Gaeta, L. Portinale, M. Minichino, and E. Ciancamerla (2003). Sequential application of heterogeneous models for the safety analysis of a control system: a case study. *Reliability Engineering and System Safety 82*(3), 269–280.

Bobbio, A., S. Montani, and L. Portinale (2003). Parametric dependability analysis through Probabilistic Horn Abduction. In *Proc. 19th Conference on Uncertainty in Artificial Intelligence*, Acapulco.

Bobbio, A., L. Portinale, M. Minichino, and E. Ciancamerla (2001). Improving the analysis od dependable systems by mapping Fault Trees into Bayesian Networks. *Reliability Engineering and System Safety 71*(3), 249–260.

Bobbio, A. and D. C. Raiteri (2004). Parametric fault-trees with dynamic gates and repair boxes. In *Proceedings Reliability and Maintainability Symposium RAMS2004*.

Doyle, S., J. Dugan, and A. Patterson-Hine (1995). A combinatorial approach to modeling imperfect coverage. *IEEE Transactions on Reliability 44*, 87–94.

Dugan, J. B., S. Bavuso, and M. Boyd (1992). Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on Reliability 41*, 363–377.

Dugan, J. B., S. Bavuso, and M. Boyd (1993). Fault-trees and Markov models for reliability analysis of fault-tolerant digital systems. *Reliability Engineering and System Safety 39*, 291–307.

Dugan, J. B., K. Sullivan, and D. Coppit (2000). Developing a low-cost high-quality software tool for dynamic fault-tree analysis. *IEEE Transactions on Reliability 49*(1), 49–59.

Garribba, S., E. Guagnini, and P. Mussio (1985). Multiple-valued logic trees: meaning and prime implicants. *IEEE Transactions on Reliability 34*, 463–472.

Heckermann, D. and M. Wellman (1995). Bayesian networks. *Communications of the ACM 38*(3), 27–30.

Jensen, F. (2001). *Bayesian Networks and Decision Graphs*. Springer.

Langseth, H. (2002). Bayesian networks with application in reliability analysis. Technical Report PhD Thesis, Dept. of Mathematical Sciences, Norvegian University of Science and Technology.

Manian, R., D. Coppit, K. Sullivan, and J. Dugan (1999). Bridging the gap between systems and dynamic fault tree models. In *Proceedings IEEE Annual Reliability and Maintainability Symposium*, pp. 105–111.

Montani, S., L. Portinale, and A. Bobbio (2004). Dynamic Bayesian Networks for modeling advanced Fault Tree features in dependability analysis. Technical Report TR-INF-03-04, Dipartimento di Informatica, Universita' del Piemonte Orientale. http://www.di.unipmn.it/Tecnical-R/index.htm.

Neapolitan, R. (1990). *Probabilistic Reasoning in Expert Systems*. J. Wiley.

Ou, Y. and J. B. Dugan (2000). Sensitivity analysis of modular dynamic fault trees. In *Proceedings International Computer Performance and Dependability Symposium*, Chicago, pp. 35–45. IEEE Computer Society Press.

Pearl, J. (1989). *Probabilistic Reasoning in Intelligent Systems*. Morgan Kaufmann.

Poole, D. (1994). Probabilistic horn abduction and bayesian networks. *Artificial Intelligence 64*(1), 81–129.

Portinale, L. and A. Bobbio (1999). Bayesian Networks for dependability analysis: an application to digital control reliability. In *Proc. 15th Conference on Uncertainty in Artificial Intelligence*, Stockholm, pp. 551–558.

Solano-Soto, J. and L. Sucar (2001). A methodology for reliable system design. In *Lecture Notes in Computer Science*, Volume 2070, pp. 734–745. Springer.

Torres-Toledano, J. and L. Sucar (1998). Bayesian networks for reliability analysis of complex systems. In *Lecture Notes in Artificial Intelligence 1484*. Springer Verlag.

Wood, A. (1985). Multi-state block diagrams and fault trees. *IEEE Transactions on Reliability 34*, 236–240.